Example $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$

$\langle (2+i) \rangle = \{(a+i)(a+ib) : a+ib \in \mathbb{Z}[i]\}$

$\mathbb{Z}[i]/\langle (2+i) \rangle = \{0+A, 1+A, 2+A, 3+A, 4+A\}$

$x+iy+A = (x+iy)(2+i) + A$

$= x(2) - 2y + A$

$(2+i)(2-i) = 5 \in A$

$k+A = k(5) + A$

$= r + A$

Example $\mathbb{Z}_3[x]/\langle x^2+1 \rangle$

$A = \langle x^2+1 \rangle = \{(x^2+1)f(x) : f(x) \in \mathbb{Z}_3[x]\}$

$= \{ax+b+A : a,b \in \mathbb{Z}_3\}$ 9 elements.

$(ax+b+A) + (cx+d+A) = (a+c)x + (b+d) + A$

$\mathbb{Z}_3$.

$(ax+b+A)(cx+d+A)$

$= acx^2 + (ad+bc)x + bd + A$

$= acx^2 + (ad+bc)x + bd - ac(x^2+1) + A$

$= (ad+bc)x + (bd-ac) + A \in \mathbb{Z}_3$.

Questions in Quiz on Thurs. will be from Homework 9 & 10

Theorem 15.5 Let R be a ring with unity. Then $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$ ($1+1+\cdots+1$) is a ring homomorphism. In particular, $\phi(\mathbb{Z}) \cong \mathbb{Z}$ or $\mathbb{Z}_n$. In the former case, R has characteristic 0; in the latter case R has characteristic n.

Corollary (a) $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\phi(a) = [a]$ is a ring homomorphism. Special case when $R = \mathbb{Z}_n$

(b) If R is a field of characteristic p, then $\{n \cdot 1 : n \in \mathbb{Z}\}$ is isomorphic to $\mathbb{Z}_p$. Special case $|\phi(1)|$ the characteristic of $R \neq$ which is a field, which in turns is an integral domain, so $|\phi(1)|$ is a prime.

Proof: Define

$\phi : \mathbb{Z} \to R$. ← unity of R.

$\phi(n) = n \cdot 1 = 1 + \cdots + 1$ if $n \in \mathbb{N}$ (n terms)

$\phi(0) = 0$ ← zero in R.

$\phi(-n) = -(1 + \cdots + 1)$ (n terms) ← additive inverse

$\phi(m+n) = (m+n) \cdot 1 = m \cdot 1 + n \cdot 1$ ✓

$\phi(mn) = (mn) \cdot 1 = (m \cdot 1)(n \cdot 1)$

$(1 + \cdots + 1) = (1 + \cdots + 1)(1 + \cdots + 1)$ (mn terms; m terms; n terms)

ring elements; ring distributive law.

Check all case $m, n \in$ positive, 0, negative

$\phi(\mathbb{Z}) = \{n \cdot 1 : n \in \mathbb{Z}\}$ is a subring of R.

[redacted]

The subgroup structure will yield $\phi(\mathbb{Z}) \cong \mathbb{Z}$ or $\mathbb{Z}_n$ where $|n| = |1|$ in the group context.

$\langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\}$

$\langle 1 \rangle = \{1 \cdot r : r \in R\}$

Definition $A \subseteq R$ is a maximal ideal if there is no ideal B of R such that $A \subsetneq B \subsetneq R$.

Fact: If A is a max ideal of a commutative ring with unity, then R/A is a field.

Construction of finite field

Theorem Suppose $\mathbb{F}$ is field, and $A = \langle f(x) \rangle \in \mathbb{F}[x]$ is a maximal ideal, where

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0.$$

Then $A = \{f(x)q(x) : q(x) \in \mathbb{F}[2]\}$, and $\mathbb{F}[x]/A = \{r(x) + A : r(x) \in \mathbb{F}[x]$ of degree at most $m-1\}$ is a field. If $\mathbb{F} = \mathbb{Z}_p$ and $f(x)$, then $\mathbb{F}[x]/A$ has p^m elements.

Example. $\mathbb{Z}_3[x]$, $A = \langle x^2+1 \rangle = \{(x^2+1)g(x) : g(x) \in \mathbb{Z}_3[x]\}$

$= \langle f(x) \rangle$.

$A_2 = \langle x^2+x+2 \rangle$

To construct a finite field with $n = p^r$ elements, where p is a prime, $r \in \mathbb{N}$,

we consider $\mathbb{Z}_p[x]/A$ where $A = \langle a_0 + \cdots + a_r x^r \rangle$ so that A is maximal.

$A \subsetneq B \subsetneq R$

$\| \quad \|$

$\langle f(x) \rangle \quad \langle g(x) \rangle$

Remark.

1° for every $r \in \mathbb{N}$ there is an irreducible monic polynomial $g(x)$ of degree r. So that $A = \langle g(x) \rangle$ is maximal.

2° $\mathbb{Z}_p[x]/A$

$= \{b_0 + b_1 x + \cdots + b_{r-1}x^{r-1} + A : b_0, b_1, \ldots, b_{r-1} \in \mathbb{Z}_p\}$

is a field with p^r elements.

Question When is $A = \langle f(x) \rangle$ maximal if $f(x) \in \mathbb{F}[x]$?

3° All finite fields, up to isomorphism is $\mathbb{Z}_p[x]/A$ with p^r elements.

Example:

$\mathbb{Z}_2[x]/A$

$A = \langle x^3+x+1 \rangle$

$\neq$

$(x+a)(x^2+bx+c)$

$\mathbb{Z}_2[x]/A$

$= \{a_0 + a_1 x + a_2 x^2 + A : a_0, a_1, a_2 \in \mathbb{Z}_2\}$

is a field with 8 elements.

Construction of the fields of quotients

Theorem 15.6 Let $\mathbb{D}$ be an integral domain. Then $(a,b) \sim (c,d)$ on $\mathbb{D} \times \mathbb{D}^*$ defined by $ad = bc$ is an equivalence relation. Suppose $\mathbb{F} = \{[(a,b)] : (a,b) \in \mathbb{D} \times \mathbb{D}^*\}$ is the set of equivalence classes of the relation. Then $\mathbb{F}$ is a field under the operations $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ and $[(a,b)][(c,d)] = [(ab, cd)]$. This is known as the field of quotients of $\mathbb{D}$.

Examples $\mathbb{D} = \mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}_p[x]$ for a prime p, and $\mathbb{R}[x]$.

Whole idea: Consider $\mathbb{D} = \mathbb{Z}, \longrightarrow \mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \right\}$ is a field.

In general, we do the following

Let $\mathbb{D}$ be an integral domain.

Consider $\mathbb{D} \times \mathbb{D}^* = \{(a,b) : a \in \mathbb{D},\ b \in \mathbb{D}^*\}$

Define an equivalence relation on $\mathbb{D} \times \mathbb{D}^*$ by

$(a,b) \sim (c,d)$ if $ad = bc$

$\mathbb{F} = \{[(a,b)] : (a,b) \in \mathbb{D} \times \mathbb{D}^*\}$

Define $[(a_1,b_1)] + [(a_2,b_2)] = [(a_1b_2 + a_2b_1, b_1b_2)]$

$[(a_1,b_1)][(a_2,b_2)] = [(a_1a_2, b_1b_2)]$

$\mathbb{D} = \mathbb{R}[x]$: $f(x)$, $g(x)$; $\mathbb{D} = \mathbb{Z}_3[x]$

(R1) $[(0,1)]$ is the additive identity, for $[(a,b)] \in \mathbb{F}$, $[(-a,b)]$ is the additive inverse.

$\mathbb{D}$ is a commutative ring $\Rightarrow (\mathbb{F}, +)$ is Abelian

$[(a,b)] + [(c,d)] = [(cb) + (ab)]$

$[(\quad bd)]$

(R2) Associative under multiplication

(R3) Distributive $(+, \cdot)$

$(\mathbb{F}^*, \cdot)$ is an Abelian group.

(G0) $(\mathbb{F}^*, \cdot)$ is closed, (G1) $\equiv$ (R2) (G2): $[(1,1)]$ is a unity

$\forall [(a,b)] \in \mathbb{F}^*$, $[(b,a)]$ is the multiplicative inverse (G4) $(\mathbb{F}^*, \cdot)$ is Abelian.